REMARKS/ARGUMENTS

The Office Action has been carefully considered. In the Office Action, claims were rejected in the following manner.

1. Claims 1-4, 8, 9, 11-19, 31, 34-36, 38, 39, 41, 42, 45-52, 54, 56, 57, 59, 60 and 61 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Nonaka et al's US Publication No. 2003/0046238 (hereinafter "*Nonaka*") in view of Hall et al's US Patent No. 7,062,500 (hereinafter "*Hall*") and further in view of Hardy et al's US Patent No. 6,079,018 (hereinafter "*Hardy*") and Thoma et al's US Publication No. 2002/0152393 (hereinafter "*Thoma*").
2. Claims 5 and 6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka, Hall, Hardy, Thoma*, and further in view of Serret-Avila et al's US Patent No. 6,959,384 (hereinafter "*Serret-Avila*").
3. Claims 10, 32, 33, 43 and 58 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka, Hall, Hardy, Thoma* and further in view of Chase Jr. et al's US Patent No. 7,080,043 (hereinafter "*Chase*").

35 U.S.C. § 103(a) Rejections

Claims 1-4, 8, 9, 11-19, 31, 34-36, 38, 39, 41, 42, 45-52, 54, 56, 57, 59, 60 and 61

Claims 1-4, 8, 9, 11-19, 31, 34-36, 38, 39, 41, 42, 45-52, 54, 56, 57, 59, 60 and 61 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka* in view of *Hall* and further in view of *Hardy* and *Thoma*.

To establish a *prima facie* case of obviousness, an Office Action must demonstrate that all claimed elements are taught or suggested by proffered prior art references. Section 2143.03 of the MPEP requires the "consideration" of every claim feature in an obviousness determination. To render a claim unpatentable, however, the Office must do more than merely "consider" each and every feature for this claim. Instead, the asserted combination of cited references must also teach or suggest *each and every claim feature*. *See In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974) (emphasis added) (to establish *prima facie* obviousness of a claimed invention, all the claim features must be taught or suggested by the prior art).

The failure of an asserted combination to teach or suggest each and every feature of a claim remains fatal to an obviousness rejection under 35 U.S.C. § 103, despite any recent revision to the MPEP. For example, in *In re Wada and Murphy,* Appeal 2007-3733, the BPAI specifically states that:

> "When determining whether a claim is obvious, an examiner must make "a searching comparison of the claimed invention – *including all its limitations* – with the teaching of the prior art." *In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995) (emphasis added). Thus, "obviousness requires a suggestion of all limitations in a claim." *CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003) (*citing In re Royka*, 490 F.2d 981, 985 (CCPA 1974)). Moreover, as the Supreme Court recently stated, "*there must be some articulated reasoning* with some rational underpinning to support the legal conclusion of obviousness." *KSR Int'l v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007) (quoting In re Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006) (emphasis added))."

In sum, it remains well-settled law that obviousness requires **at least a suggestion of all of the elements of a claim**. *See In re Wada and Murphy*, *citing CFMT, Inc. v. Yieldup Intern. Corp.*, 349 F.3d 1333, 1342 (Fed. Cir. 2003) and *In re Royka*, 490 F.2d 981, 985 (CCPA 1974)). Moreover, it is "important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements **in the way the claimed new invention does**." *KSR*, 127 S.Ct. at 1741.

Applicant respectfully submits that the elements of the current claims are not taught or suggested by *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, and that *Nonaka, Hall, Hardy* and *Thoma* fail to teach or suggest combination of the elements of the current claims **"in the way the claimed new invention does."**

For example, Claim 1 reads:

1. (Previously Presented) A method comprising:

obtaining clear form rights information at a client device, said clear form rights information being associated with content stored at said client device;

obtaining **a clear form external integrity hash of first data comprising:**

said clear form rights information and

an external key as an integrity secret;

obtaining **an internal integrity hash of second data comprising**

said clear form rights information,

said clear form external integrity hash, and

an externally inaccessible client device key;

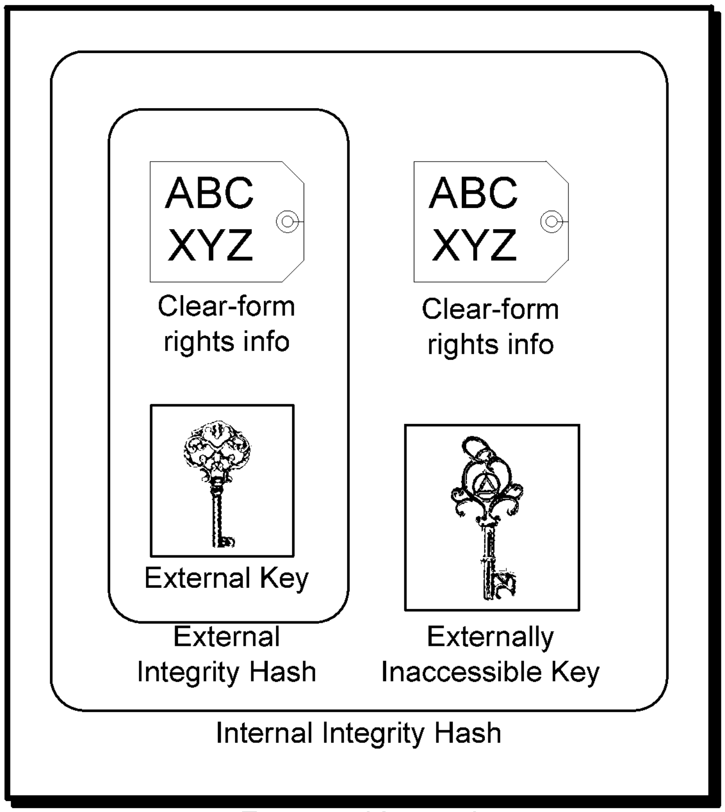
encrypting said internal integrity hash using said externally inaccessible client device key; and storing the encrypted internal integrity hash on the client device.

Accordingly, Claim 1 is directed to an encrypted hash that comprises (1) clear-form rights information; (2) an externally inaccessible key; and (3) a clear-form hash, which comprises (a) the clear-form rights information and (b) an external key. Applicant asserts that *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, fail to teach of suggest an encrypted hash having the above elements. However, even if *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, suggest a hash having the above elements, *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, fail to suggest such a hash "**in the way the claimed new invention does.**"

Nonaka, Hall, Hardy and Thoma fail to teach or suggest the elements of Claim 1

While, *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, may teach various elements of Claim 1, **all** elements are not taught or suggested. For example, Claim 1 is directed to an encrypted internal integrity hash, which comprises clear-form rights information, and which further comprises a hash comprising **the same** clear-form rights information. In other words, there is a hash of a hash of the clear-form rights information, which also includes the same clear-form rights information. This is a concept that is simply not taught or suggested by *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination.

For example, the figure below is a representation of the encrypted hash of Claim 1:



Encrypted Internal
Integrity Hash of Claim 1

As shown above, the encrypted integrity hash comprises two copies of the clear-form rights information. Specifically, a first copy of the rights information is in the external hash, and a second copy of the rights information is in the internal integrity hash (which also includes the external integrity hash).

Nonaka, Hall, Hardy and *Thoma,* either alone or in combination, fail to teach or suggest an encrypted internal integrity hash having two copies of clear-form rights information as depicted above, and the Office Action fails to establish a *prima facie* case of obviousness relating to the concept of two copies of clear-form rights information.

For example, the Office Action cites *Hardy* as teaching a "hash generated from a previous hash and an encryption key." (Office Action, page 6) Even if *Hardy* teaches or suggests such a concept, *Hardy* nonetheless fails to teach or suggest a second hash generated from (1) rights information; (2) an encryption key; and (3) a first hash that itself comprise (a) **the same rights information as in the second hash**, and (b) an external key. Applicant has reviewed *Nonaka, Hall, Hardy* and *Thoma,* alone and collectively, and fails to find a teaching or suggestion of such a hash. Additionally, even if *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, successfully teaches or suggests some elements of the encrypted hash of Claim 1 depicted above, *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, fails to teach or suggest the encrypted hash of Claim 1 **as a whole** or **"in the way"** recited by Claim 1.

Nonaka, Hall, Hardy and Thoma fail to teach or suggest Claim 1 as a whole or teach or suggest the elements of Claim 1 in the same way.

Although *Nonaka, Hall, Hardy* and *Thoma,* teach various hashing techniques, and hashes of various keys and rights information, *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination fail to teach or suggest Claim 1 as a whole or in the same way as recited in Claim 1.

Additionally, the Office Action only addresses some elements of Claim 1, and certainly does not address Claim 1 as a whole. For example, the Office Action asserts that "*Hall* discloses: (b) obtaining a clear form external integrity hash of first data comprising said clear form rights information; (c) obtaining an internal hash of second data comprising said clear form rights information." (Office Action, page 8) However, the Office Action provides an incomplete recitation of the relevant portions of Claim 1. Specifically, the following depicts the relevant portions of Claim 1 that are not included:

> "*Hall* discloses: (b) obtaining a clear form external integrity hash of first data comprising said clear form rights information [**and an external key as an integrity secret**]; (c) obtaining an internal hash of second data comprising said clear form rights information [**said clear form external integrity hash, and an externally inaccessible client key**]."

The emphasized portions added above appear to be elements of Claim 1 that are essentially ignored in the Office Action. The Office Action, on pages 8-9, does however assert the following, which appears to confuse the first internal and external hashes:

> Nonaka-Hall does not specifically disclose a hash comprising a hash and an encryption key. However, Hardy discloses wherein a hash comprising said clear form rights information and an external key as an integrity secret. (see Hardy col. 10, lines 56-64: combines the digest H (previously generated hash), with signer's private key; concatenate two values; hash generated from a previous hash and a private key)

Here, the Office Action cites teaching an element of the "external integrity hash" (i.e. "wherein a hash comprising said clear form rights information and an external key as an integrity secret"), yet seems to intend to refer to an element of the "internal integrity hash" when citing *Hardy*. Specifically, the Office Action asserts *Hardy* teaches a "hash comprising a hash and an encryption key," which appears to be an assertion of *Hardy* teaching the "internal integrity hash" of Claim 1.

Regardless, the Office Action fails to address a hash comprising a hash of a hash, wherein the first hash includes rights information and an external key. Moreover, the Office Action fails to address a hash of a hash wherein the first and second hash both comprise the same clear-form rights information. Such concepts are not taught or suggested by *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, and even the portions that are asserted to be taught would not teach or suggest Claim 1 as a whole.

For example, as discussed above the Office Action, on pages 8-9 asserts the following:

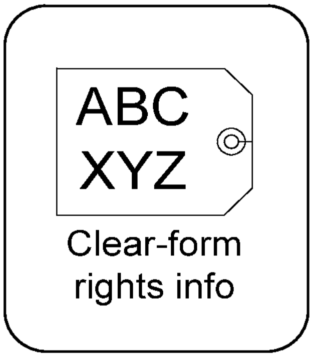
> *Hall* discloses: (b) obtaining a clear form external integrity hash of first data comprising said clear form rights information; (c) obtaining an internal hash of second data comprising said clear form rights information....
>
> Nonaka-Hall does not specifically disclose a hash comprising a hash and an encryption key... (see Hardy col. 10, lines 56-64: combines the digest H (previously generated hash), with signer's private key; concatenate two values; hash generated from a previous hash and a private key)

Accordingly, the Office Action asserts that *Nonaka, Hall, Hardy* and *Thoma,* either alone or in some combination, teach the following, which are depicted below:

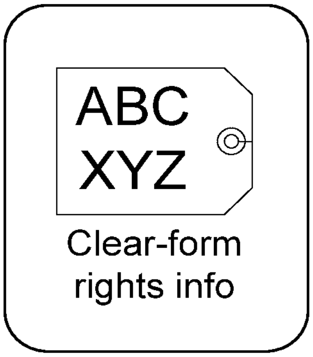
(1) "obtaining a clear form external integrity hash of first data comprising said clear form rights information."

(2) "obtaining an internal hash of second data comprising said clear form rights information."

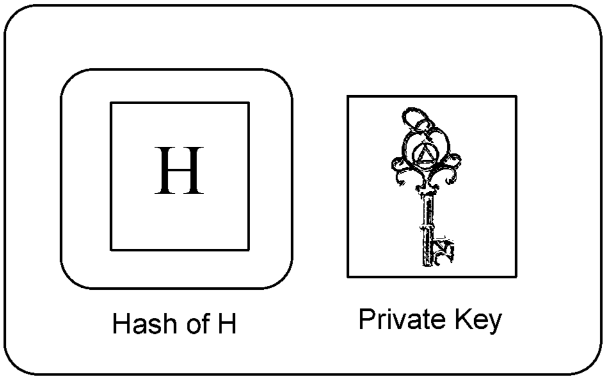
(3) "Hardy col. 10, lines 56-64: combines the digest H (previously generated hash), with signer's private key; concatenate two values; hash generated from a previous hash and a private key."



External Hash

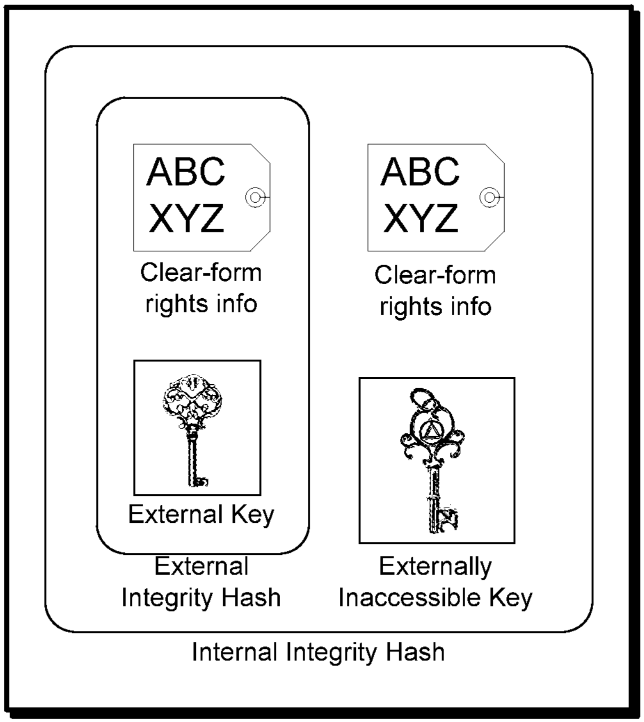


Internal Hash



Hash of Digest H and
Private Key

Even if any of *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, teach the elements depicted above (which Applicant specifically argues that they do not), a teaching of the above elements certainly does not teach or suggest the elements of Claim 1, which is depicted below. *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, fail to remedy these teaching deficiencies discussed above, and the Office Action does not address or remedy such teaching deficiency. Applicant has reviewed *Nonaka, Hall, Hardy* and *Thoma* in depth, both alone and in combination, and simply cannot find a teaching or suggestion of the elements of Claim 1 as a whole, which are depicted below:



Encrypted Internal
Integrity Hash of Claim 1

Accordingly, Applicant respectfully asserts that Claim 1 is patentable over *Nonaka, Hall, Hardy* and *Thoma,* either alone or combined, and that Claim 1 is in condition for allowance along with Claims 2-4, 8, 9, and 11-19, which depend therefrom.

Claims 2-4, 8, 9, 11-19, 31, 34-36, 38, 39, 41, 42, 45-52, 54, 56, 57, 59, 60 and 61

Claims 2-4, 8, 9, 11-19 depend from allowable Claim 1 and are therefore allowable at least by dependency. However, Claims 2-4, 8, 9, 11-19 are also patentable because *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, fail to teach or suggest elements of Claims 2-4, 8, 9, 11-19.

For example Claim 9 reads:

> The method of claim 1 further comprising:
>
> generating a validation hash from at least the clear form rights information;
>
> decrypting the encrypted internal integrity hash to recover the internal integrity hash; and
>
> **comparing the validation hash to the internal integrity hash to detect tampering with the rights information**.

Accordingly, Claim 9 is directed to obtaining and comparing a validation hash and an encryption hash to determine whether rights information has been tampered with. The Office Action asserts that the elements of Claim 9 are taught by *Nonaka*. For example, the Office Action asserts that paragraph [0246] teaches "**comparing the validation hash to the internal integrity hash to detect tampering with the rights information.**" However, a close reading of paragraph [0246] and proximate paragraphs illustrates that the elements of Claim 9 are not taught by *Nonaka*. Specifically, paragraphs [0243-0246] read:

> [0243] The directory structure data represents a relationship among the content files CF and a relationship between the content file CF and the key file KF within the secure container 104.
>
> [0244] For example, if content files CF_1 through CF_3 and the corresponding key files KF_1 through KF_3 are stored in the secure container 104, a link between the CF_1 through CF_3 and a link between the content files CF_1 through CF_3 and the key files KF_1 through KF_3 are established, as shown in FIG. 9, by the directory structure data.
>
> [0245] The hyperlink data represents a hierarchical structure of the key file KF and a relationship between the content files CF and the key files KF by considering all the files inside and outside the secure container 104.

> [0246] More specifically, address information to be linked and the authentication value (hash value) thereof are stored, as shown in FIG. 10, in the secure container 104 for each content file CF and for each key file KF. **The hash value of one content file CF or one key file KF obtained by a hash function H (x) is then compared with that of another file CF or another key file KF to be linked, thereby verifying the link between the files.**

Here, *Nonaka* merely discloses comparing hashes of key files, content files, or a key file and a content file to verify a link between such files. This, however, is not a teaching or suggestion of comparing a generated hash and retrieved hash to determine whether the contents of the retrieved hash have been tampered with. Moreover, the cited portion of *Nonaka* above fails to disclose generating and decrypting as recited in Claim 1, and the sections of *Nonaka* that are cited to teach other elements of Claim 9 fail to remedy this teaching deficiency because such sections fail to relate to the CF and KF files of the paragraphs excerpted above. The sections cited by the Office Action, which allegedly teach the various elements of Claim 9, **do not relate to each other** and it appears that the cited sections were chosen simply because of keywords therein.

In another example, the elements of Claim 13 are not taught or suggested by *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination. Claim 13 reads:

> The method of claim 1 wherein the clear form rights information comprises usage information, the method further comprising:
>
> tracking usage of the content;
>
> updating the clear form rights information with changes in usage; and
>
> for each update of the clear form rights information:
>
> **re-obtaining the internal integrity hash of second data comprising the updated clear form rights information, said clear form external integrity hash, and said externally inaccessible client device key**; and
>
> re-encrypting, and re-storing the internal integrity hash on the client device.

Accordingly, Claim 13 relates to re-generating an integrity hash comprising (1) rights information; (2) an encryption key; and (3) a first hash that itself comprises (a) **the same rights information as in the second hash**, and (b) an external key. As discussed above, *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, fail to teach or suggest generating the integrity hash of Claim 1 a first time, and therefore cannot teach or suggest re-generating the same hash as recited in Claim 13 a second time. The portions of *Nonaka, Hall,* and *Hardy* cited in the Office Action, which allegedly teach the elements of Claim 13, fail to remedy this teaching deficiency.

In another example, the elements of Claim 15 are also not taught or suggested by *Nonaka, Hall, Hardy* and *Thoma*, either alone or in combination. Claim 15 reads: "…wherein the client device key comprises a code embedded in hardware of the client device having no externally accessible data path." In contrast, paragraphs [0036] and [0346] of *Nonaka*, which are alleged to teach Claim 15, fail to teach or suggest the elements of Claim 15. Specifically, *Nonaka* fails to teach a "client device" comprising a "code embedded in hardware" having "no externally accessible data path." Paragraph [0346] does teach "the SAM" being "completely shielded from an external source," but the "SAM" as described in this paragraph does not refer to a client device key, or a code that comprises a client device key as in Claim 15. *Nonaka, Hall, Hardy* and *Thoma* do not remedy this teaching deficiency, either alone or in combination, and therefore Claim 15 is in condition for allowance.

Accordingly, Applicant respectfully asserts that Claims 2-4, 8, 9, 11-19 are patentable over *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, and therefore Claims 2-4, 8, 9, 11-19 are in condition for allowance.

Additionally, Independent Claims 31, 34 and 49 comprise elements analogous to elements in Claim 1 and are patentable over *Nonaka, Hall, Hardy* and *Thoma,* either alone or in combination, for at least the same reason as Claim 1. Claim 33 depends from Claim 31; Claims 35-36, 38, 39, 41, 42, and 45-48 depend from Claim 31 and Claims 50-52, 54, 56, 57, 59, 60 and 61 depend from claim 49. Accordingly Claims 33-36, 38, 39, 41, 42, 45-48, 50-52, 54, 56, 57, 59, 60 and 61 are in condition for allowance at least by dependence.

Claims 5 and 6

Claims 5 and 6 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka, Hall, Hardy, Thoma*, and further in view of *Serret-Avila*. Claims 5 and 6 depend from Claim 1, which is in condition for allowance based on the reasons discussed above and therefore Claims 5 and 6 are also allowable at least by dependency. Additionally, the elements of Claims 5 and 6 are not taught by *Nonaka, Hall, Hardy, Thoma*, or *Serret-Avila*, either alone or in combination.

For example, the Office Action asserts that *Nonaka* teaches "receiving the external key at the client device." However, as then identified by the Office Action, *Nonaka* merely teaches "**storing** the integrity hash on the client device." *Nonaka,* does not teach obtaining an external key, or integrity hash from an external source and therefore does not teach **receiving**.

Accordingly, Claim 5 is patentable over *Nonaka, Hall, Hardy, Thoma*, and *Serret-Avila*, either alone or in combination.

<u>Claims 10, 32, 33, 43 and 58</u>

Claims 10, 32, 33, 43 and 58 were rejected under 35 U.S.C. § 103(a) as being unpatentable over *Nonaka, Hall, Hardy, Thoma* and further in view of *Chase*. Claim 10 depends from allowable Claim 1; Claims 32 and 33 depend from allowable Claim 31; Claim 43 depends from allowable Claim 34; and Claim 58 depends from allowable Claim 49. Therefore Claims 10, 32, 33, 43 and 58 are in condition for allowance based at least on dependency.

Additionally, the elements of Claims 10, 32, 33, 43 and 58 are not taught by *Nonaka, Hall, Hardy, Thoma* or *Chase*, either alone or in combination. For example, the Office Action asserts that "disabling the content of the client device if tampering is detected" is taught by *Chase.* This element, as in Claims 10, 32, 33, 43 and 58, is however, not taught or suggested by *Chase* (or *Nonaka, Hall, Hardy, Thoma,* either alone or in combination).

The Office Action seems to mistakenly cite *Chase,* col. 4, lines 10-16, which allegedly teaches "content compromised such as tampering, access to content disabled." A close reading of *Chase,* col. 4, lines 10-16 reveals that tampering is not being detected, and that a license is merely being selectively modified by the system. Specifically, *Chase,* col. 4, lines 13-15, teaches that the *Chase* system "determines based on the content revocation whether such license **is to be** disabled or otherwise affected"

Importantly, the determination here is being made whether the license will be "disabled or otherwise affected" **by the system**. This is not the same as determining whether tampering has occurred to the license. Accordingly, Claims 10, 32, 33, 43 and 58 are patentable over *Hall, Hardy, Thoma* and *Chase*, either alone or in combination.

CONCLUSION

For at least the reasons above, Applicant respectfully submits that all pending claims are allowable and request that the Examiner permit these claims to proceed to issuance. Although additional arguments are believed to exist for distinguishing the cited documents, the arguments presented are believed sufficient to address the Examiner's rejections. Likewise, failure of the Applicant to respond to a position taken by the Examiner is not an indication of acceptance or acquiescence of the Examiner's position. Instead, it is believed that the Examiner's positions are rendered moot by the foregoing arguments, and it is therefore not believed necessary to respond to every position taken by the Examiner with which Applicant does not agree.

The Examiner is respectfully requested to contact the undersigned at the telephone number below if there are any remaining questions regarding this application.

We believe the appropriate fees accompany this transmission. If, however, insufficient fee payment or fee overpayment occurs, the amount may be withdrawn or deposited from/to AXIOS Law Group's deposit account. The deposit account number is 50-4051.

Respectfully submitted,
AXIOS LAW GROUP

Date: July 8, 2009

by: /Adam L.K. Philipp/

Adam L.K. Philipp - Reg. No.: 42,071
Direct: 206.217.2226
E-mail: adam@axioslaw.com

AXIOS Law Group
1525 4th Avenue, Suite 800
Seattle, WA 98101
Telephone: 206-217-2200
Customer No.: 61,857